Spegni & Riaccendi S.p.A.

PREVENTIVO DI INSTALLAZIONE NETWORK

SPEGNI&RIACCENDI SPA

Mail: spegnietriaccendi@hotmail.it

01 – PREMESSA

In data 15.12.2025 alle ore 9,15 ca. la COMPAGNIA THETA affidava a Spegni&Riaccendi S.p.a di sviluppare un Preventivo di Spesa per la configurazione della loro rete aziendale.

Nello specifico a Spegni&Riaccendi S.p.a veniva richiesto di:

- ✓ **Progettare infrastruttura IT;**
- ✓ **Progettare un piano di Sicurezza Perimetrale;**
- ✓ **Progettare Servizi di Supporto;**

02 – REQUISITI

Qui vengono elencati i dettagli tecnici e i parametri richiesti da COMPAGNIA THETA.

L'edificio nella quale si compone la COMPAGNIA THETA possiede **Piani 6;**

Sono previsti:

- Computers 20 per Piano, per un totale di numero 120 Computers

Componenti aggiuntivi richiesti:

- **Switch** (Collega più dispositivi all'interno di una rete locale)
- **Router** (dispositivo che collega più reti, permettendo a tutti di condividere la stessa connessione)
- **Firewall Perimetrale** (controllo del traffico in entrata/uscita e blocca minacce della rete)
- **DMZ** (Demilitarized Zone, sistema di sicurezza che crea rete separata per ospitare server pubblici proteggendo la rete interna da potenziali attacchi)
- **Web Server** (Sistema hardware e software che memorizza, elabora e distribuisce contenuti Web tramite richieste HTTP)
- **IDS/IPS** (Ispeziona pacchetti rete, rileva e invia avvisi di minacce e/o rileva e blocca minacce)

Mail: spegnietriaccendi@hotmail.it

03 – ELENCO DISPOSITIVI E QUANTITA'

A seguito viene riportata una tabella nella quale vengono elencati la tipologia, specifiche tecniche e quantità dei Computers proposti da SPEGNI&RIACCENDI SPA.

Elementi della tabella:

- **TIPOLOGIA**: Indica il Dispositivo Computers (HARDWARE)
- **AREA:** Indica l'Area Lavorativa per la quale è pensato il Dispositivo Computer, divisa in Amministrativa e Progettuale.
- **SO:** Indica il Sistema Operativo installato con Licenza d'Uso (SOFTWARE)
- **CPU:** Central Processing Unit. Il Processore, responsabile delle istruzioni software (HARDWARE)
- **RAM:** Random Access Memory, memoria temporanea utilizzata dal Sistema Operativo e dai programmi in esecuzione, riferita in Gb (Gigabytes) (HARDWARE)
- **SSD:** Memoria di archiviazione per immagazzinare programmi Software e Dati, riferita in Gb (Gigabytes) o Tb (Terabytes) (HARDWARE)
- **QUANTITA':** Numero dei Dispositivi Computers proposti in questa configurazione, vengono inserite le quantità riferite ad un Piano dell'edificio della COMPAGNIA THETA, preso come esempio, e si riproporrà nei 5 Piani restanti.

TIPOLOGIA	AREA	SO	CPU	RAM	SSD	QUANTITA'
Computer	**Amministrativa Commerciale Segreteria**	**Windows11 Pro Microsoft Corp**	**Intel i5**	**16 Gb**	**512 Gb**	**90**
Computer	**Progettuale Management**	**Windows11 Pro Microsoft Corp**	**Intel i7**	**32 Gb**	**1 Tb**	**30**

*N.B.: I **Computers** dedicati all'**AREA Progettuale** sono dotati di una **GPU** (Graphic Processal Unit) integrata marca **NVIDIA RTX 3060** che gestisce la grafica e accellera il rendering dell'immagini.

Nella prossima vengono elencati i Dispositivi necessari per la configurazione della **RETE** proposti da **SPEGNI&RIACCENDI SPA**

Elementi della tabella:

Mail: spegnietriaccendi@hotmail.it

- **TIPOLOGIA:** Indica il tipo di Dispositivo (HARDWARE E/O SOFTWARE) installato
- **MODELLO:** Indica la Modello del Dispositivo (HARDWARE E/O SOFTWARE) installato
- **QUANTITA':** Numero dei Dispositivi necessari per questa configurazione di **Rete** (HARDWARE E/O SOFTWARE) installati

TIPOLOGIA	MODELLO	QUANTITA'
Switch	**NETGEAR Switch Ethernet 48 Porte Unmanaged GS348**	**8**
Router	**ROUTER WLAN CISCO FPR1120-ASA-K9**	**1**
Firewall	**Cisco ASA5512-IPS-K9 firewall**	**2**
WEB SERVER	**DELL PowerEdge T40 server 1000 GB Mini Tower Intel Xeon E 3,5 GHz 8 GB DDR4-SDRAM 550HK**	**1**
NAS	**UGREEN NASync DXP4800 Plus**	**1**
IDS/IPS	**Greed® Nano Plus - i5 10400** **Powerful Mini PC**	**3**
CABLAGGIO 1	**Cavo ethernet Cat6**	**305 m x 12 scatole**

04–INFRASTRUTTURA DI RETE

SPEGNI&RIACCENDI SPA propone una **infrastruttura di rete** progettata con l'**obiettivo di garantire sicurezza, affidabilità, scalabilità** e soprattutto una **facile gestione**.

Mail: spegnietriaccendi@hotmail.it

Separa in modo chiaro le diverse **Aree** funzionali delle **Reti LAN** (rete aziendale destinata ai client interni), **DMZ** (area destinata ai servizi esposti verso l'esterno) e **WAN** (connessione a internet e reti esterne)

Questa netta separazione consente di **ridurre gli attacchi** verso la rete e **applicare policy di sicurezza.**

COMPONENTI PRINCIPALI DELL'INFRASTRUTTURA

In questa sezione introdurremo le VLAN, una Rete logica che segmenta la Rete fisica in più sottoreti isolati migliorando Sicurezza e Prestazioni, Access, collegamenti via cavo ai Dispositivi, e Trunk collegamenti via cavo tra gli Switch e Router

1. **Firewall perimetrale:**

- ✓ Rappresenta il primo livello di difesa della rete
- ✓ Gestisce il traffico in ingresso e in uscita tramite regole di filtraggio
- ✓ Consente l'accesso controllato ai servizi pubblici presenti nella DMZ
- ✓ Posto tra la rete WAN e l'infrastruttura

2. **Router centrale:**

- ✓ Si occupa dell'instradamento del traffico tra le diverse reti interne
- ✓ Consente una gestione centralizzata dei flussi tra LAN, DMZ e servizi interni
- ✓ Collocato nella parte inferiore del Firewall

3. **Firewall interno:**

- ✓ Rappresenta il secondo livello di difesa della rete
- ✓ Gestisce il traffico in ingresso e in uscita tramite regole di filtraggio
- ✓ Posto tra la Router Centrale e lo Switch Centrale

4. **Switch centrale (Core Switch)**

- ✓ Trasporta il traffico delle diverse VLAN tramite collegamenti (collegamenti Trunk)
- ✓ Permette una struttura scalabile e facilmente estendibile
- ✓ Punto di aggregazione di tutti gli Switch nei Piani dell'edificio

Mail: spegnietriaccendi@hotmail.it

5. **Switch dei Piani dell'edificio**

- ✓ Ogni piano è dotato di uno Switch
- ✓ Gli HOST (Dispositivi Computers, Server, etc). sono collegati tramite Porte Access alla VLAN del Piano, permettendo l'isolamento del traffico e la facile gestione.

6. **IDS/IPS interni**

- ✓ Consentono il monitoraggio del traffico e l'individuazione di attività anomale e/o malevoli
- ✓ Rafforzano la sicurezza interna, lavorando con il Firewall perimetrale
- ✓ Vengono posizionati in punti strategici della rete

SEGMENTAZIONE DELLA RETE

Viene segmentata la LAN interna tramite VLAN, una per ciascun piano, con indirizzamento IP (Internet Protocol) dedicato. Questa segmentazione permette di:

- ✓ Isolare i domini di broadcast;
- ✓ Limitare la propagazione di eventuali attacchi interni;
- ✓ Applicare Policy di sicurezza e controllo del traffico.

SICUREZZA A PIÙ LIVELLI

- Filtraggio perimetrale tramite Firewall
- Separazione dei servizi pubblici nella DMZ;
- Segmentazione della LAN interna;
- Monitoraggio del traffico tramite IDS/IPS;
- Controllo centralizzato dei flussi tra le diverse aree della rete.

Questo approccio riduce il rischio che una singola vulnerabilità comprometta l'intero sistema.

LOGICA DELLE REGOLE DI SICUREZZA (POLICY)

Mail: spegnietriaccendi@hotmail.it

La configurazione seguirà lo standard di Sicurezza Internazionale **"Default Deny"** (Nega tutto per difetto).

Qui verranno strutturare le REGOLE:

- **Blocco Predefinito:** Di base, tutto il traffico è bloccato, Nessuno può entrare o uscire se non esplicitamente autorizzato.
- **Regole di Ingresso (Inbound):**
  1. Dall'esterno verso la Rete Interna:
     BLOCCATO: Nessun accesso diretto ai PC.
  2. Dall'esterno verso la DMZ:
     PERMESSO: Solo per i servizi strettamente necessari

- **Regole di Uscita (Outbound):**
  1. Dalla Rete Interna verso Internet:
     FILTRATO: I dipendenti potranno navigare, *ma* l'accesso a siti pericolosi o malware sarà bloccato dai filtri di sicurezza.

- **Regole tra DMZ e LAN:**
  1. Dalla DMZ verso la Rete Interna:
     BLOCCATO. I server pubblici non possono iniziare connessioni verso i **Dati Privati**.

IMPLEMENTAZIONE DELLA ZONA DMZ (DEMILITARIZED ZONE)

Per proteggere i dati sensibili dell'Azienda, SPEGNI&RIACCENDI configurerà una **DMZ.**

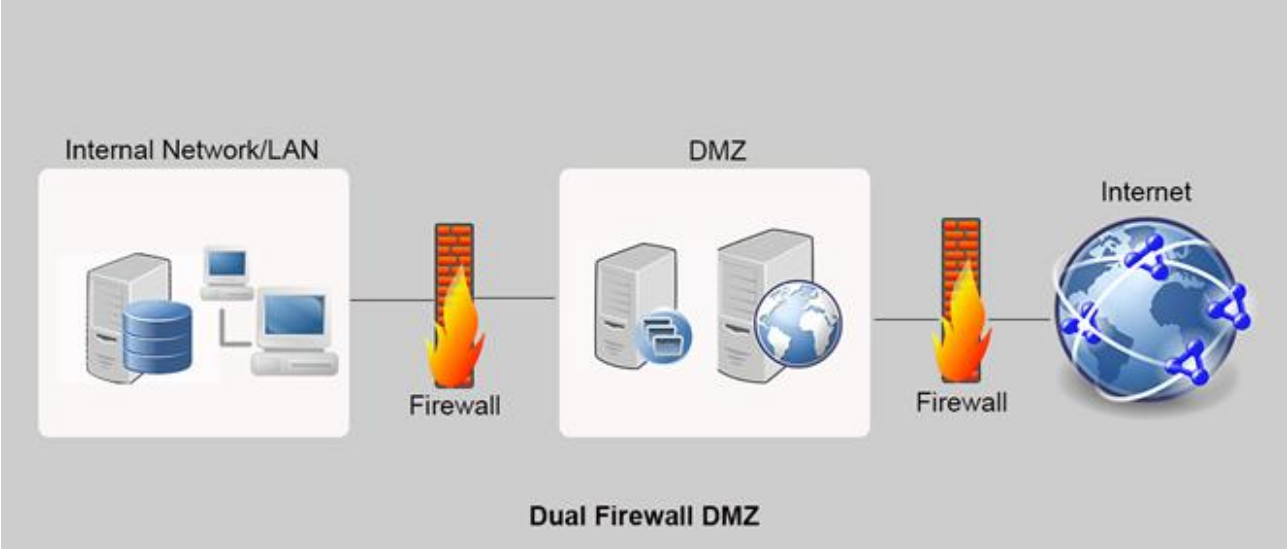
- La **LAN (Rete Interna):** È la “cassaforte” dove risiedono i vostri dati privati, i PC dei dipendenti e il server gestionale.

- La **DMZ (Zona “Cuscinetto”):** È come la "Reception" o l'atrio. Qui posizioneremo i servizi che devono essere accessibili dall'esterno (es. server web, portali clienti, o servizi di posta pubblica).

Il Vantaggio di Sicurezza:

*Qualora un attaccante dovesse riuscire a violare un servizio pubblico nella **DMZ**, rimarrebbe confinato nella **DMZ** (es. Reception), le porte per la "cassaforte" (la vostra **Rete Interna/LAN**), rimarrebbero **CHIUSE E BLOCCATE** dal **FIREWALL.***

Mail: spegnietriaccendi@hotmail.it



05 - SERVIZI DI INSTALLAZIONE

La presente sezione descrive la soluzione infrastrutturale proposta da SPEGNI&RIACCENDI SPA, e le attività che verranno eseguite per la realizzazione, configurazione e integrazione dell'infrastruttura di Rete del Cliente, con particolare attenzione alla segmentazione logica, alla gestione centralizzata e alla SICUREZZA del traffico.

L'architettura è progettata secondo principi di separazione dei ruoli, sicurezza multilivello e scalabilità, in linea con le best practice di progettazione adottate nelle infrastrutture di rete aziendali.

5.1 POSA E ATTESTAZIONE CABLAGGIO STRUTTURATO

Il Servizio di Posa del Cablaggio strutturato comprende le attività necessarie alla messa in esercizio dell'Infrastruttura di Rete passiva già predisposta all'interno dell'edificio, articolato su sei piani.

In particolare, il Servizio prevede:

- Attestazione dei cavi di rete esistenti sui patch panel di piano;
- Realizzazione dei collegamenti fisici tra patch panel e porte di rete degli apparati installati;
- Organizzazione e instradamento ordinato dei cablaggi all'interno dei rack;

- Etichettatura delle tratte e verifica della continuità delle connessioni.

Le Attività sono finalizzate a rendere il cablaggio strutturato esistente pienamente operativo e pronto per le successive fasi di configurazione della Rete.

5.2 CONFIGURAZIONE SWITCH E VLAN

SPEGNI&RIACCENDI SPA propone la realizzazione di una segmentazione logica dell'infrastruttura di Rete basata su VLAN, finalizzata a garantire isolamento del traffico, ordine architetturale e facilità di gestione.

La SOLUZIONE prevede la configurazione degli SWITCH di Accesso e dello SWITCH centrale per supportare:

- VLAN dedicate per ciascun piano dell'edificio;
- una VLAN di management per la gestione centralizzata;
- una VLAN dedicata ai servizi di storage (NAS).

Segmentazione per piani

Per ogni Piano dell'Edificio è prevista una VLAN dedicata, all'interno della quale sono collocati i dispositivi degli utenti.
Le Porte degli switch di piano saranno configurate in modalità Access, assicurando l'associazione fisica dei dispositivi alla VLAN corretta, mentre i collegamenti verso lo Switch Centrale saranno configurati in modalità Trunk per il trasporto delle VLAN necessarie.

Le VLAN Utente **adottano indirizzamento IP dinamico (DHCP)**, consentendo una gestione semplificata dei dispositivi e garantendo flessibilità e scalabilità dell'infrastruttura nel tempo.

Tabella VLAN 101-106 (di piano)

Nome VLAN	ID VLAN	Subnet	Netmask	Gateway	Assegnazione IP
Piano1	101	192.168.101.0/26	255.255.255.192	192.168.101.1	**DHCP** – 192.168.101.20 → 192.168.101.62

Piano2	102	192.168.102.0/26	255.255.255.192	192.168.102.1	**DHCP** – 192.168.102.20 → 192.168.102.62
Piano3	103	192.168.103.0/26	255.255.255.192	192.168.103.1	**DHCP** – 192.168.103.20 → 192.168.103.62
Piano4	104	192.168.104.0/26	255.255.255.192	192.168.104.1	**DHCP** – 192.168.104.20 → 192.168.104.62
Piano5	105	192.168.105.0/26	255.255.255.192	192.168.105.1	**DHCP** – 192.168.105.20 → 192.168.105.62
Piano6	106	192.168.106.0/26	255.255.255.192	192.168.106.1	**DHCP** – 192.168.106.20 → 192.168.106.62

VLAN di Management

La soluzione proposta include una **VLAN di management dedicata**, utilizzata esclusivamente per la gestione degli apparati di rete e dei servizi infrastrutturali.

All'interno della VLAN di management sono previsti:

- Apparati di Routing;
- SWITCH centrali e di piano;
- Dispositivi di Sicurezza;
- Servizi Infrastrutturali di Supporto.

Gli indirizzi IP assegnati alla VLAN di management sono statici, al fine di garantire:

- Raggiungibilità costante degli apparati;
- Stabilità operativa;
- Semplicità nelle attività di amministrazione, monitoraggio e troubleshooting.

L'accesso alla **VLAN di Management** non è vincolato alla posizione fisica all'interno dell'edificio, ma avviene tramite meccanismi di accesso logico controllato.

La SOLUZIONE PROPOSTA DA SPEGNI&RIACCENDI S.P.A. **prevede** che il personale del reparto IT *possa gestire gli apparati di rete da qualsiasi area operativa, sfruttando il routing inter-VLAN e specifiche policy di sicurezza configurate sul router/firewall centrale*.

In particolare, l'accesso alla **VLAN di Management** è consentito esclusivamente a HOST **autorizzati**, identificati tramite **Regole di controllo del traffico** (ACL), mentre tutte le altre VLAN Utente risultano bloccate verso la Rete di Gestione.

Mail: spegnietriaccendi@hotmail.it

A tale livello di filtraggio si affianca l'AUTENTICAZIONE sugli apparati di Rete tramite Protocolli sicuri, GARANTENDO che anche in presenza di traffico autorizzato l'accesso sia consentito solo a personale abilitato.

Questo approccio consente di mantenere la **VLAN di Management** completamente isolata dal traffico Utente, EVITANDO la necessità di punti di accesso fisici dedicati e adottando un modello di sicurezza a difesa stratificata, in linea con le best practice delle infrastrutture di Rete Aziendali.

Nome VLAN	ID VLAN	Subnet	Netmask	Gateway	Assegnazione IP
Management	50	192.168.50.0/26	255.255.255.192	192.168.50.1	**Statico** – indirizzi dedicati apparati di rete (vedi tabella Management)

Tabella VLAN 100 – Management (indirizzi statici)

Nome VLAN	Ruolo	Indirizzo IP
Router	Gateway VLAN Management	192.168.50.1
Switch centrale	Gestione core	192.168.50.2
Switch piano 1	Gestione access	192.168.50.3
Switch piano 2	Gestione access	192.168.50.4
Switch piano 3	Gestione access	192.168.50.15
Switch piano 4	Gestione access	192.168.50.6
Switch piano 5	Gestione access	192.168.50.7
Switch piano 6	Gestione access	192.168.50.8
NAS (gestione)	Amministrazione NAS	192.168.50.9
Firewall Perimetrale	Gestione sicurezza	192.168.100.1
Firewall Interno	Gestione sicurezza	192.168.150.1
IDS 1	Monitoraggio perimetrale / DMZ	192.168.50.60

Mail: spegnietriaccendi@hotmail.it

IDS 2	Monitoraggio traffico interno	192.168.50.61
IPS 1	Protezione NAS	192.168.50.62

VLAN 100 – Management (indirizzi statici)

5.3 INTEGRAZIONE NAS

SPEGNI&RIACCENDI S.P.A. **propone l'integrazione di un sistema di Network Attached Storage (NAS)** dedicato al backup dei dati di lavoro degli utenti e al supporto delle attività infrastrutturali.

Il NAS è collocato in una **VLAN dedicata ai servizi di storage**, separata sia dalle VLAN Utente sia dalla VLAN di Management, al fine di distinguere in modo chiaro:

- l'accesso ai dati;
- l'accesso amministrativo al sistema.

Gli utenti possono accedere al NAS esclusivamente per le operazioni di backup tramite protocollo **SMB**, mentre l'accesso di configurazione e amministrazione del dispositivo è consentito unicamente dalla VLAN di management.

VLAN 90 – NAS (indirizzi)

Nome VLAN	ID VLAN	Subnet	Netmask	Gateway	Assegnazione IP
NAS	90	192.168.90.0/26	255.255.255.192	192.168.90.1	**Statico** – 192.168.90.10

La separazione tra traffico utente e traffico di gestione consente di aumentare il livello di sicurezza e di preservare l'integrità dei servizi infrastrutturali.

5.4 INTEGRAZIONE IDS/IPS

Mail: spegnietriaccendi@hotmail.it

SPEGNI E RIACCENDI S.P.A. **propone l'integrazione di sistemi di Intrusion Detection e Intrusion Prevention (IDS/IPS)** come parte integrante dell'architettura di sicurezza dell'infrastruttura di rete.

I sensori **IDS/IPS** saranno collocati in punti strategici dell'infrastruttura al fine di consentire:

- il monitoraggio del traffico tra rete interna e perimetro di sicurezza;
- l'analisi del traffico in prossimità della DMZ e dei servizi esposti;
- il controllo del traffico interno per l'individuazione di comportamenti anomali.

La SOLUZIONE prevede la configurazione delle connessioni necessarie all'analisi dei flussi di traffico, la verifica del corretto funzionamento dei sensori e l'allineamento con le policy di sicurezza definite per l'infrastruttura.

L'integrazione dei sistemi IDS/IPS, in combinazione con la segmentazione VLAN, consente l'adozione di un **approccio di sicurezza a difesa stratificata**, migliorando la visibilità sugli eventi di sicurezza e riducendo l'impatto di potenziali minacce.

In seguito verrano installate le Regole di filtraggio del traffico implementate sull'apparato di Sicurezza Perimetrale.

La configurazione sarà progettata seguendo il principio del **"Least Privilege" (Minimo Privilegio)**, garantendo che ogni utente o servizio abbia accesso esclusivamente alle risorse necessarie per il proprio lavoro, riducendo drasticamente la superficie di attacco.

1. **Politica di Base: "Default Deny" (Blocco Preventivo)**

In conformità con gli standard di sicurezza più elevati, la regola fondamentale del **FIREWALL** è impostata su **BLOCK (Blocco Totale)**.

Interfaccia	Protocollo	Action	Source	Destination	Port
WAN					
	Any	Block ❌	Any	Any	Any

La seguente Figura mostra la regola del Firewall e l'Azione di Blocco

Mail: spegnietriaccendi@hotmail.it

Il **FIREWALL** non permette alcun traffico a meno che non sia esplicitamente autorizzato.

- **Principale Vantaggio:**
  Qualora un attaccante tentasse di scansionare la rete o qualora un servizio interno venisse compromesso, il **FIREWALL** agisce come un "muro di fuoco", impedendo non autorizzati verso la Rete Sensibile (192.168.100.x).

2. Gestione degli Accessi Interni (Segmentazione della Rete)

Abbiamo suddiviso la Rete Aziendale in zone logiche distinte, applicando regole specifiche per ogni gruppo di Utenti come dettagliato nella configurazione attuale:

- **Accesso Management (Super-User):**

  È stata creata una **Regola Privilegiata** per la **Rete di Gestione** (Management Net).
  Gli Amministratori avranno accesso completo **TCP/UDP** (Protocolli di Trasporto delle Informazioni) verso la zona **DMZ**. Questo garantisce il pieno controllo operativo su **Server Web, Switch** e infrastruttura di **FIREWALLING**

- **Accesso Sviluppatori (Restricted Access):**

  Per la rete Sviluppatori sarà applicata una regola restrittiva.
  A differenza del Management, gli Sviluppatori potranno accedere **esclusivamente all'indirizzo del Web Server** (IP finale 192.168.100.5) per le attività di manutenzione del sito.

  - ✓ **SICUREZZA**: È esplicitamente impedito loro l'accesso ad altri apparati critici (come l'interfaccia del **FIREWALL** o dello **SWITCH**), **proteggendo l'infrastruttura** da errori umani o accessi non necessari e/o non autorizzati.

Mail: spegnietriaccendi@hotmail.it

- **Protezione Utenti Standard:**
  Tutti gli altri utenti della rete **LAN** (Piani 1-6) sono **bloccati** dall'accesso alla **DMZ**. Questo impedirà che un dipendente non autorizzato possa inavvertitamente manomettere i Server Pubblici.
  Garantisce il solo accesso verso Internet per la normale operatività.

Interfaccia	Protocollo	Action	Source	Destination	Port
LAN (tra DMZ_net e theta_net)					
	TCP / UDP	Pass ✅	192.168.100.0/26 (Management Net)	172.16.1.0/29 (DMZ net)	Any
	TCP / UDP	Pass ✅	192.168.106.0/26 ("Sviluppatori" Net)	172.16.1.5 (Web Server)	Any
	Any	Block ❌	LAN net (101.x,102.x,...,105.x)	172.16.1.0/29 (DMZ net)	Any
	Any	Pass ✅	LAN net (101.x,102.x,...,106.x)	Any	Any

La seguente Figura mostra la regola del Firewall e l'Azione di Accesso controllato

3. Gestione della Zona Pubblica (DMZ) e Web Server

La configurazione della Demilitarized Zone (DMZ), regola il traffico verso, e dal Vostro sito web:

- **Visibilità Pubblica:** Dall'esterno (WAN).
  L'unica porta aperta sarà la **Porta 80** verso il Web Server. Questo renderà il **sito raggiungibile dai clienti**, mantenendo **chiuse tutte le altre porte di servizio.**

Interfaccia	Protocollo	Action	Source	Destination	Port
WAN					
	Any	Pass ✅	Any	172.16.1.5	80

La seguente Figura mostra la regola del Firewall e l'Azione di Accesso controllato

Mail: spegnietriaccendi@hotmail.it

- **Auto-Protezione del Firewall:**
  Sarà implementata una **Regola** di Sicurezza Critica ("Anti-Lockout/Anti-Hack"). Qualora il **Web Server** dovesse essere compromesso da un Hacker, una **Regola** specifica **BLOCCHEREBBE** qualsiasi tentativo del server di accedere all'interfaccia di gestione del FIREWALL (Porte 443/80/22 verso l'IP 192.168.100.6).

  ✓ **RISULTATO:**
  L'attaccante rimane isolato sul Server Web e non potrà prendere il controllo della Rete Aziendale.

Interfaccia	Protocollo	Action	Source	Destination	Port
LAN (verso DMZ_net)					
	Any	Block ✗	LAN net	172.16.1.6	443/80/22
	Any	Pass ✓	LAN net	Any	Any

La seguente Figura mostra la regola del Firewall e l'Azione di Blocco e Accesso

06 - DETTAGLI ATTIVITA'

In questa Fase Operativa, il Team Tecnico di SPEGNI&RIACCENDI, utilizzerà i NOSTRI Strumenti SOFTWARE Esclusivi e Personalizzati, per convalidare l'Integrità della Rete e la SICUREZZA dei sistemi installati:

1. **VERIFICATORE PROTOCOLLI WEB (HTTP Verb Tester)**

   Questo Strumento è dedicato al collaudo del **Web Server** Aziendale. Serve a verificare che il Server comunichi CORRETTAMENTE e in modo SICURO con l'esterno.

   a. **FUNZIONE**: Invia diverse tipologie di richieste al Server per controllare come reagisce

b. **SEMPLICITA' D'USO**: Dispone di un'Interfaccia guidata che permette ai tecnici di impostare facilmente l'indirizzo IP da testare

c. **RISULTATO:** Produce un Report finale in formato testo che riassume quali operazioni sono permesse e quali sono bloccate, GARANTENDO che il Server non esponga vulnerabilità.

2. **SCANNER DI SICUREZZA DELLE PORTE (Port Scanner)**

Questo Strumento viene utilizzato per MAPPARE i Dispositivi in Rete e VERIFICARE l'efficacia del **FIREWALL PERIMENTRALE.**

a. **FUNZIONE:** CONTROLLA se un Dispositivo Computer è acceso e ANALIZZA quali PORTE di comunicazione ha aperte.

b. **OBIETTIVO:** ASSICURARE che solo le PORTE (necessarie al lavoro) siano accessibili, chiudendo tutte le altre per evitare intrusioni.

c. **FUNZIONAMENTO**: ESEGUE una Scansione rapida e SEGNALA in tempo reale al Tecnico lo STATO delle Porta (Aperta/chiusa) di ogni punto di Accesso Testato

3. **ANALIZZATORE DI TRAFFICO DI RETE (Packet Sniffer)**

a. **FUNZIONE:** INTERCETTA i Pacchetti di Dati che viaggiano tra i vari Dispositivi
b. **DETTAGLI:** VISUALIZZA in tempo reale l'origine e la destinazione di ogni comunicazione (Indirizzi IP e MAC

c. **UTILITA':** Strumento fondamentale DIAGNOSTICA i problemi di connessione e VERIFICA che i sistemi **IDS/IPS** stiano rilevando correttamente il traffico di rete

Mail: spegnietriaccendi@hotmail.it

07 - PREZZO

TIPOLOGIA	MODELLO	QUANTITA'	PREZZO	TOTALE
Computer	**Lenovo ThinkStation P360Tower IntelCore i7**	**30**	**1600,00 cad**	**48000 €**
Computer	**Lenovo ThinkStation P360 IntelCore i5 16GB**	**90**	**800,00 cad**	**72000 €**

TIPOLOGIA	MODELLO	QUANTITA'	PREZZO	TOTALE
Switch	**NETGEAR Switch Ethernet 48 Porte Unmanaged GS348**	**8**	**300,00 cad.**	**2400,00 €**
Router	**ROUTER WLAN CISCO FPR1120-ASA-K9**	**1**	**2300,00 cad**	**2300,00 €**
Firewall	**Cisco ASA5512-IPS-K9 firewall**	**2**	**2400,00 cad.**	**2400,00 €**
WEB SERVER	**DELL PowerEdge T40 server 1000 GB Mini Tower Intel Xeon E 3,5 GHz 8 GB DDR4-SDRAM 550HK**	**1**	**800,00 cad.**	**800,00 €**

Mail: spegnietriaccendi@hotmail.it

NAS	**UGREEN NASync DXP4800 Plus**	**1**	**600,00 cad.**	**600,00 €**
IDS/IPS	**Greed® Nano Plus - i5 10400 Powerful Mini PC**	**3**	**650,00 cad.**	**1950,00 €**
CABLAGGIO 1	**Cavo ethernet Cat6**	**305 m x 12 scatole**	**300,00**	**3600,00 €**

TOTALE	**131650,00 €**

08 - ONORARIO SERVIZI

A SPEGNI&RIACCENDI S.P.A. è riservato un Onorario per i Servizi resi pari euro 3000,00 (tremila) al giorno + IVA. Il tempo necessario per l'Implementazione e Configurazione della RETE per la COMPAGNIA THETA, è stimato in 21 (ventuno) giorni lavorativi.

Allo scadere dei 21 giorni stimati per il completamento della Configurazione SPEGNI&RIACCENDI S.P.A. offre un SERVIZIO DI SUPPORTO TOTALMENTE GRATUITO nei successivi 30(trenta) giorni lavorativi, COME SPECIFICHERA' IL CONTRATTO DI INGAGGIO.

ONORARIO SERVIZI	GIORNI	TOTALE
3000,00 €	21	63000 €

DISPOSITIVI	**131650 € +IVA**
ONORARIO	**63000 €**

TOTALE	**194650 €**

SPEGNI&RIACCENDI S.P.A